

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-242470

(P2000-242470A)

(43) 公開日 平成12年9月8日 (2000.9.8)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 7/58		G 0 6 F 7/58	A 5 J 1 0 4
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00	6 5 0 B
H 0 4 L 9/24		H 0 4 L 9/00	6 5 7

審査請求 未請求 請求項の数5 O L (全 8 頁)

(21) 出願番号 特願平11-44365

(22) 出願日 平成11年2月23日 (1999.2.23)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 樋口 淑夫

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100097445

弁理士 岩橋 文雄 (外2名)

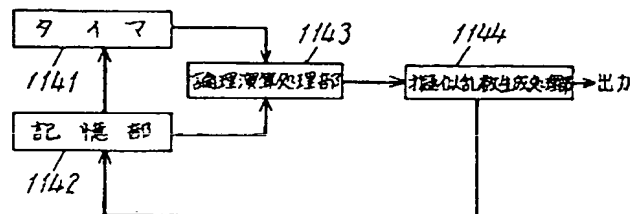
Fターム(参考) 5J104 FA00 GA03 GA04 NA04 NA35

(54) 【発明の名称】 乱数生成装置および方法および記録媒体

(57) 【要約】

【課題】 乱数生成の際に必要なシード値を装置内部で自動的に生成し、外部からの解析にも強固な乱数を生成する。

【解決手段】 装置の起動時、タイマ1141に記憶部1142からデータを転送し、タイマ1141の計数を開始する。乱数生成時、タイマ1141の計数値と記憶部1142のデータを用いて論理演算処理部1143で論理演算を行い、演算結果を初期シード値として、擬似乱数生成処理部1144の初期値として入力することにより出力に乱数が得られる。生成した乱数の一部を記憶部1142にフィードバックする。



【特許請求の範囲】

【請求項1】 タイマの値と記憶部が格納するデータ値からシード値を生成する論理演算処理部と、前記シード値から乱数を生成する擬似乱数生成処理部と、を備えることを特徴とする乱数生成装置。

【請求項2】 前記記憶部は、生成した乱数をフィードバックして保持することを特徴とする請求項1記載の乱数生成装置。

【請求項3】 前記タイマは、動作開始時に前記記憶部が格納するデータ値を開始点として計数することを特徴とする請求項1記載の乱数生成装置。

【請求項4】 記憶部からデータを取得し、取得したデータをタイマの開始点として計数を行う計数処理手段と、記憶部からデータを取得し、前記タイマと前記取得データからシード値を生成する論理演算処理手段と、前記シード値から乱数を生成する擬似乱数生成処理手段と、前記乱数を前記記憶部にフィードバックして記録する記録処理手段と、を備えることを特徴とする乱数生成方法。

【請求項5】 記憶部からデータを取得し、取得したデータをタイマの開始点として計数を行う計数処理手段と、前記記憶部からデータを取得し、前記タイマと前記取得データからシード値を生成する論理演算処理手段と、前記シード値から乱数を生成する擬似乱数生成処理手段と、前記乱数を前記記憶部にフィードバックして記録する記録処理手段と、を備えることを特徴とする乱数生成プログラムを格納した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、自分自身で電源を持たない回路および装置上で、自動的に乱数を生成する乱数生成装置および方法および記録媒体に関するものである。

【0002】

【従来の技術】 近年、情報通信システムの発展とともに、データ通信の安全性を高めるセキュリティ技術の重要性が高まっている。なかでも、乱数生成技術は安全なデータ通信を保証するために利用する暗号化技術には不可欠なものであり、主な用途として、ワンタイムパスワードの作成、暗号化に使用する鍵値の作成、暗号文の生成、電子署名情報の生成等がある。

【0003】 暗号化技術を利用すれば、データの暗号化、および、本人認証に必要な電子署名の生成を行うことができる。これらの技術は、処理性能の高いパーソナルコンピュータやワークステーションなどのデスクトップコンピュータ上で行われてきていたが、電子マネーやIDカードによる個人用途向けのセキュリティシステム

等で利用するために、ICカード上に実装したマイクロコンピュータにおいて乱数を生成し、暗号化技術を利用する必要性が生じている。

【0004】 従来より、回路および装置を用いて乱数の生成を行う場合には、物理手段を利用して乱数列を発生させる方式と数学的な演算処理を行い、長周期の乱数列を生成する擬似乱数生成方式の2種類の方式を用いている。さらに、通信のセキュリティを確保するための暗号化技術においても、このようにして生成された乱数が用いられているが、電子マネーやIDカード等の個人向けのセキュリティ用途で使用する場合には、乱数生成方式の実用性と生成した乱数の安全性が特に重要になってくる。

【0005】 物理手段を利用して乱数列を発生させる多数の方式が知られている。以下、物理手段を利用して乱数を発生させる方式について述べる。この例としては、抵抗体の熱雑音により乱数を生成する方式があげられる。抵抗体の熱雑音は多数の電子により発生する微少電流を合成したものであり、それぞれの電子の衝突・散乱は無関係に発生するため、雑音は一樣に発生する。高抵抗の両端に発生する微少な雑音電圧を、ハイインピーダンス・低雑音のアンプで増幅して雑音電圧を取得し、その電圧をA/Dコンバータでデジタルデータに変換してパーソナルコンピュータやワークステーションに入力、棄却法やくくり合わせ法などの処理を行うことによって、乱数の性質の改善を行うことができ、適切な乱数が得られる。

【0006】 この方式は、物理的な性質を利用するので、0と1の発生確率がおのおの約1/2になり、各ビットが他の部分と独立であるので、生成される乱数列の推測は困難であり、セキュリティの用途に適した乱数列が得られるが、特別なハードウェアを必要とするので非常にコストがかかり、特に、マイクロコンピュータ上に実装しての利用には不向きである。

【0007】 擬似乱数生成方式として多数の方式が知られている。以下、擬似乱数生成方式により乱数を生成する方式について述べる。この例としては、線形フィードバックシフトレジスタによる方式があげられる。図8は線形フィードバックシフトレジスタの例であり、201はシフトレジスタのセル、202は排他的論理和回路、203はシフトレジスタの出力である。出力される乱数列は、シフトレジスタ201の個数、排他的論理和回路202の構成によって異なり、図8に示す構成に限られるものではない。

【0008】 以上のように構成された線形フィードバックシフトレジスタについて、以下、その動作を説明する。最初に、シフトレジスタのセル201にそれぞれ初期値を設定し、シフトレジスタのセル201の内容から排他的論理和回路202により論理演算を行い、演算結果をシフトレジスタの出力203に出力する。1ビット

3

を出力するごとに、シフトレジスタのセル201のデータを矢印の方向にシフトさせていき、出力はシフトレジスタのセル201にフィードバックしてシフトを繰り返していく。この結果、 n 段を有するシフトレジスタは最大 $N=2^{n-1}$ ビット長の非周期的ビット列を生成し得ることになり、段数の多いシフトレジスタを使用すれば、長周期の擬似乱数が得られる。

【0009】この装置は、特別なハードウェアを必要とせず、ソフトウェアによる実現が可能であり、マイクロコンピュータ上で利用できるが、シフトレジスタのセル201の初期値により乱数列が生成されるためにシフトレジスタの構成およびシフトレジスタの初期値が判明すれば同様の乱数列を容易に生成し得ることが欠点である。擬似乱数生成方式として他に線形合同法、暗号技術による方法、デジタルカオス法等があげられるが、これらも同様の欠点を持っている。

【0010】したがって、擬似乱数生成方式を利用して乱数を生成するには、乱数を生成するごとに初期シード値を設定する必要がある。一般的に、パーソナルコンピュータやワークステーション上では初期シード値として、システムが保有している現在時刻が用いられている。

【0011】

【発明が解決しようとする課題】しかしながら、非接触型のICカードのような内部で現在時刻などのリアルタイムに変化するデータを持っていないシステムでは、外部から初期シード値を供給する必要がある。図9は外部から初期シード値を供給して乱数を生成する一実施の形態であり、211はマイクロコンピュータ、212はマイクロコンピュータ211の外部入力、213はマイクロコンピュータ211に実装した擬似乱数生成処理部、214はマイクロコンピュータ211の外部出力である。まず、外部入力212から入力された初期シード値は、擬似乱数生成処理部213で初期シード値に設定されて乱数を生成し、外部出力214に乱数を出力する。

【0012】図9のような上記従来の構成では、外部入力212から初期シード値を盗聴することが可能であり、入出力の相関関係から内部の擬似乱数生成処理部が解析できるため、安全であるとはいえない。

【0013】本発明は、上記従来の問題点を解決するため、自分自身で電源を持たない装置上で、外部からの入力により初期シード値を設定することなく、自身で閉じて乱数を生成する乱数生成装置および方法および記録媒体を提供することを目的とする。

【0014】

【課題を解決するための手段】上述課題を解決するために、請求項1にかかる発明は、タイマの値と記憶部が格納するデータ値からシード値を生成する論理演算処理部と前記シード値から乱数を生成する擬似乱数生成処理部を備えることを特徴とする乱数生成装置としている。

4

【0015】また、請求項2にかかる発明においては、前記記憶部は、生成した乱数をフィードバックして保持することを特徴とする請求項1記載の乱数生成装置としている。

【0016】さらに、請求項3にかかる発明においては、前記タイマは、動作開始時に前記記憶部が格納するデータ値を開始点として計数することを特徴とする請求項1記載の乱数生成装置としている。

【0017】前記構成によって、起動時ごとに異なるタイマの値と記憶部に蓄積されているデータから、擬似乱数生成の際に用いる初期シード値を自動的に生成することができるので、自分自身で電源を持たない回路および装置上でも安全性の高い乱数を低コストで生成することができる。

【0018】

【発明の実施の形態】以下、本発明の一実施の形態として、乱数生成装置について説明する。なお、本実施の形態では装置による実施の形態について説明しているが、本発明は装置に限定するものではなく、ソフトウェアにより機能を実現してもよい。

(1) 乱数生成装置を用いたシステム

図1は、本実施形態における乱数生成装置を用いたシステム例として、ICカード内蔵マイクロコンピュータを用いた暗号処理システムについて説明している。図1において、10はICカード、11はICカード10に内蔵されている自身で電源を内蔵していないマイクロコンピュータ、12はICカード10とのデータの通信を行う通信機、13は通信機12の制御を行う制御機器である。まず、図1のICカード10の存在を確認後、制御機器13から通信機12に指示を与え、ICカード10に通信機12から電力を供給する。マイクロコンピュータ11は自身で電源を持たないので、通信機12から電力の供給を受けて起動、動作を行う。一方、マイクロコンピュータ11を起動後、制御機器13から、通信機12を経由して、データを伝送し、マイクロコンピュータ11において乱数を生成し、生成した乱数を利用してマイクロコンピュータ11内部で暗号処理を行う。暗号処理後のデータは、通信機器12を経由して、制御機器13に伝送される。

【0019】図2は、マイクロコンピュータ11の処理の構成をあらわすブロック図である。図2において、111はICカード10に送受信されるデータの処理を行うI/O処理部、112はマイクロコンピュータ11における処理全般の制御を行うOS処理部、113はデータの暗号化を行う暗号処理部、114は暗号化を行う際に用いる乱数を生成する乱数生成部である。ICカード10に送信されたデータはマイクロコンピュータ11で処理される。マイクロコンピュータ11においてデータは、I/O処理部111、OS処理部112で処理が行われ、暗号処理部113に渡される。一方、乱数生成部

114では、暗号処理部113から乱数の要求があった際に乱数を生成し、暗号処理部113に送る。暗号処理部113では、前記入力データを前記乱数で暗号化し、暗号化されたデータはOS処理部112を経由して、I/O処理部111に渡し、通信機12へと伝送する。

【0020】なお、本乱数生成装置は、前記実施形態に限定するものではなく、乱数の生成を必要とする電子署名生成システムにも利用できる。電子署名を生成するには、図2において、暗号処理部で行っている処理の代わりに電子署名の生成を行えばよい。

(2) 乱数生成装置の詳細

上記のように乱数は乱数生成部114で生成される。ここでは、図3は乱数生成部114の構成をあらわすブロック図を参照して説明を行う。図3において、1141はマイクロコンピュータ11の動作開始時点から乱数生成部114における乱数の生成開始時点までの時間を計測するタイマ、1142は生成した乱数をフィードバックして蓄積する記憶部、1143は乱数の初期シード値を生成する論理演算処理部、1144は初期シード値から擬似乱数を生成する擬似乱数生成処理部である。まず、タイマ1141はマイクロコンピュータ11に通信機12から電力が供給され起動した際に、記憶部1142からタイマにデータを転送し、カウンタの開始時点とする。次に、タイマ1141の計数を開始し、論理演算処理部1143での処理を開始するまで計数を継続する。なお、初回の乱数生成時には、記憶部1142にあらかじめ装置のシリアル番号等のデータを蓄積しておくといふ。乱数を生成する際には、前記タイマが計数している値と記憶部1142に蓄積されているデータを論理演算処理部1143において論理演算を行い、演算結果を初期シード値として擬似乱数生成処理部1144に入力して乱数を生成する。生成された乱数の一部または全てのデータを記憶部1142にフィードバックして以前に蓄積していたデータに上書きし、次の乱数生成時に利用する。なお、論理演算処理部1143、擬似乱数生成処理部1144における処理はハードウェア、ソフトウェアのどちらで機能を実現してもよい。

【0021】以下、図4のフローチャートを参照して、本実施の形態における乱数生成処理の概略について説明する。

(ステップS301)マイクロコンピュータ11の起動時、記憶部1142からデータを取得し、タイマ1141に転送する。その値から計数を開始し、論理演算処理部1143における論理演算の開始時まで計数を継続する。ステップS302に行く。

(ステップS302)論理演算処理部1143においてタイマ1141の計数値と記憶部1142のデータを取得し、これら2値の論理演算を行う。乱数の初期シード値を生成する。ステップS303に行く。

(ステップS303)前記初期シード値を擬似乱数生成処

理部1144に入力して乱数を得る。ステップS304に行く。

(ステップS304)前記乱数をフィードバックして記憶部1142に蓄積する。以下、図5のフローチャートを参照して、本実施の形態における乱数生成装置の動作の詳細について説明する。

(ステップS401)制御機器13からの指示を通信機12が受信し、通信機12とデータの送受信を行うICカード10が存在することを確認する。存在すれば、ステップS402に行く。存在しなければ、ステップS401に戻る。

(ステップS402)通信機12からICカード10に電力を供給する。ステップS403に行く。

(ステップS403)ICカード10は通信機12から供給された電力により、マイクロコンピュータ11を起動する。同時に、記憶部1142からタイマ1141にデータを転送し、タイマ1141は計数を開始する。ステップS404に行く。

(ステップS404)制御機器13から指示に基づき、通信機12を介在して、暗号化するデータをICカード10に伝送する。ステップS405に行く。

(ステップS405)ICカード10がデータを受信すれば、ステップS406に行く。受信できていなければ、ステップS404に戻る。

(ステップS406)暗号化を開始する指示を乱数生成部114に出す。ステップS407に行く。

(ステップS407)暗号化開始の要求を受け、起動していたタイマ1141を停止する。ステップS408に行く。

(ステップS408)タイマ1141と記憶部1142の値に対して、論理演算処理部1143で論理演算を行い、初期シード値を生成する。ステップS409に行く。

(ステップS409)初期シード値を擬似乱数生成処理部1144に入力し、乱数を得る。得た乱数は記憶部1142に蓄積しておく。ステップS410に行く。

(ステップS410)生成した乱数および受信したデータを暗号処理部113に入力、暗号化を行い、暗号化データを得る。ステップS411に行く。

(ステップS411)通信機12を介在して、暗号化データをICカード10から制御機器13に伝送する。通信機12はICカードへの電力の供給を終了する。ステップS401に戻る。

【0022】以上のように本実施形態によれば、論理演算処理部1143での演算処理を行うまでには、ICカード10と通信機12との間の通信処理時間、OS処理部112での処理時間が含まれ、これらの処理時間は処理するデータおよびシステムを実施する環境によって異なる。すなわち、乱数を生成することにタイマ1141による計数値は異なる計数値となる。さらに、タイマ1

1 4 1によって計数された値のみでは、値のバラツキが小さくなる可能性があるので、タイマ1 1 4 1における計数の開始時点の値を記憶部1 1 4 2のデータから取得するとともに、記憶部1 1 4 2のデータとの論理演算を行うことによって値のバラツキの範囲を広範囲かつ予測不可能にしている。

【0 0 2 3】外部からの解析によって、擬似乱数生成処理部1 1 4 4による擬似乱数生成方式および記憶部1 1 4 2に蓄えられているデータが判明した場合、生成される乱数が予測される可能性がある。しかし、上記で説明したようにタイマ1 1 4 1のカウンタの値は通信環境により毎回異なるので、タイマ1 1 4 1の値と記憶部1 1 4 2に蓄えられているデータの2値を用いて論理演算を行った値を正確に予測することは困難であり、この値が1ビットでも異なれば、擬似乱数生成処理部1 1 4 4はまったく異なった乱数を生成するので、外部からの解析にも強固な乱数生成装置となる。

【0 0 2 4】なお、擬似乱数生成処理部1 1 4 4で利用する方式としては線形フィードバックシフトレジスタがあげられる。他にも線形合同法、暗号技術による方法、デジタルカオス法等の初期シード値を必要とする擬似乱数生成方式により行ってもよい。

(3) 演算処理部の詳細

上記のように論理演算処理部1 1 4 3では擬似乱数生成処理部1 1 4 4への初期シード値を生成するために論理演算を行う。ここでは、図6を参照して論理演算処理部1 1 4 3の具体的な一実施形態について説明する。図6において、1 1 4 1はタイマであり、1 1 4 2は記憶部であり、1 1 4 5は排他的論理和回路、1 1 4 6は論理演算処理部1 1 4 3の出力である。まず、タイマ1 1 4 1の値は上位ビット列と下位ビット列に分割してビット列の上位部分と下位部分の位置を反転する。一方、記憶部1 1 4 2に蓄積されているデータも上位ビット列と下位ビット列に分割し、上記の反転した値とそれぞれ排他的論理和の演算を行う。次に、それぞれのビット列を再び結合して論理演算処理部1 1 4 3の出力1 1 4 6とし、この出力値を初期シード値として擬似乱数生成処理部1 1 4 4に入力し乱数を得る。

【0 0 2 5】最大周期が長いタイマを利用した際には、マイクロコンピュータ1 1の起動時から乱数生成時までの時間が極端に短い場合、タイマ1 1 4 1の上位ビットが開始時点から変化がないこともありえるが、タイマ1 1 4 1の値の上位ビット列と下位ビット列を反転することにより、最大周期が長いタイマを利用したとしても、排他的論理和の演算を行った際に出力1 1 4 6の上位ビットが全て0になることはない。なお、論理演算処理部1 1 4 3は上記の方式に限定するものではない。

(4) 記憶部内のデータ

本実施形態における記憶部1 1 4 2内の記録方式の一実

施形態を図7に示す。実施形態としては、記憶部1 1 4 2内の特定のアドレスを指定しておき、そのアドレスを開始点としてデータを蓄積すればよい。乱数生成を行うごとに同じアドレスに上書きして前回のデータを残さないようにしておくようにする。上記のように記憶することにより、暗号化の際に利用した乱数データが判明しないようにしておく。

【0 0 2 6】

【発明の効果】本発明は、タイマと擬似乱数生成処理部からデータのフィードバックを行う記憶部を利用することにより、特別なハードウェアを追加することなく、装置内部で自動的に乱数を生成できる優れた乱数生成装置および方法および記録媒体を実現するものである。

【図面の簡単な説明】

【図1】ICカードを用いた暗号処理システムの構成図

【図2】ICカード内蔵マイクロコンピュータのブロック構成図

【図3】本発明の一実施形態における構成図

【図4】本発明の乱数生成処理のフローチャート

【図5】本発明の一実施形態におけるフローチャート

【図6】本発明の一実施形態における演算処理部の構成図

【図7】記憶部内のデータに関する概略図

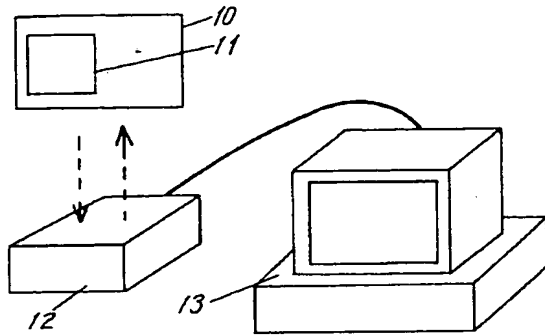
【図8】数学的な演算処理により擬似乱数列を生成する従来例の回路図

【図9】擬似乱数生成処理部を利用して乱数を生成する従来例の構成図

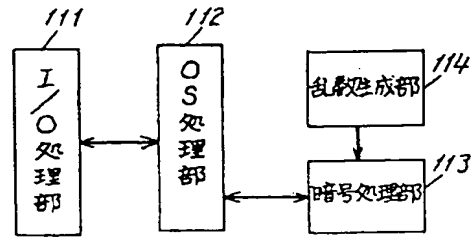
【符号の説明】

- 1 0 ICカード
- 1 1 マイクロコンピュータ
- 1 2 通信機
- 1 3 制御機器
- 1 1 1 I/O処理部
- 1 1 2 OS処理部
- 1 1 3 暗号処理部
- 1 1 4 乱数生成部
- 2 0 1 シフトレジスタのセル
- 2 0 2 排他的論理和回路
- 2 0 3 シフトレジスタの出力
- 2 1 1 マイクロコンピュータ
- 2 1 2 マイクロコンピュータの外部入力
- 2 1 3 擬似乱数生成処理部
- 2 1 4 マイクロコンピュータの外部出力
- 1 1 4 1 タイマ
- 1 1 4 2 記憶部
- 1 1 4 3 論理演算処理部
- 1 1 4 4 擬似乱数生成処理部
- 1 1 4 5 排他的論理和回路
- 1 1 4 6 論理演算処理部出力

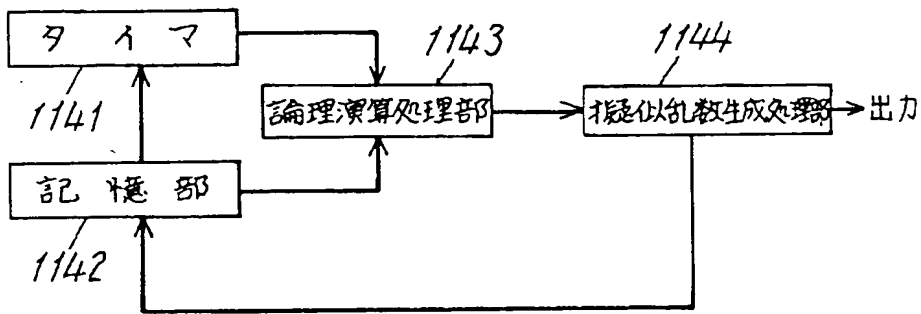
【図1】



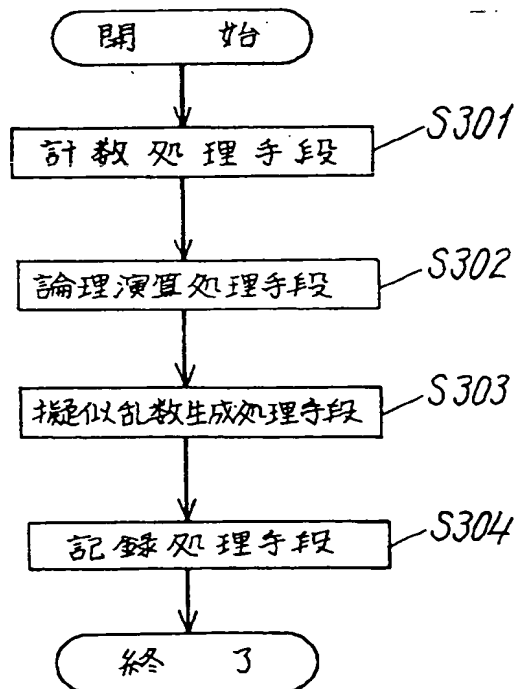
【図2】



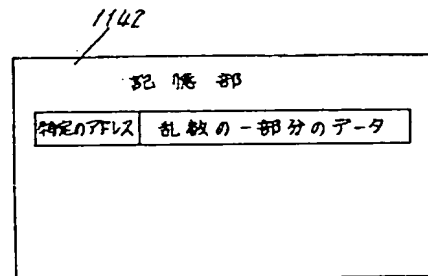
【図3】



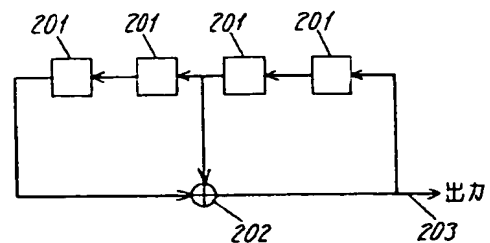
【図4】



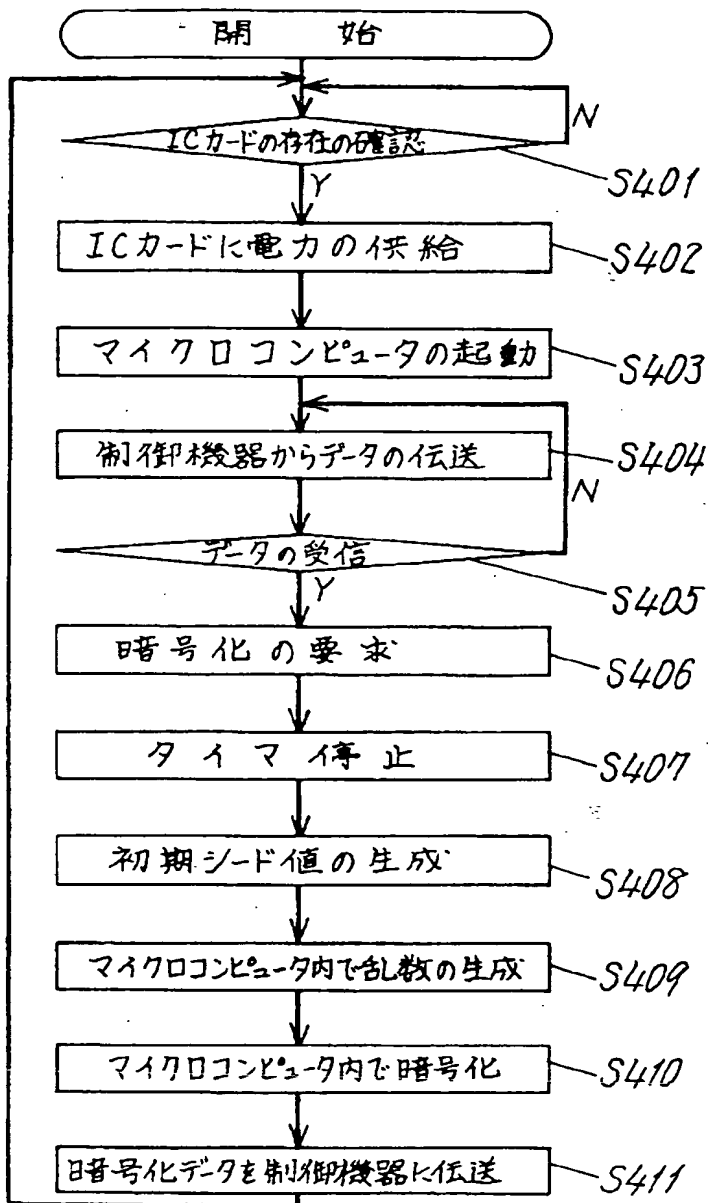
【図7】



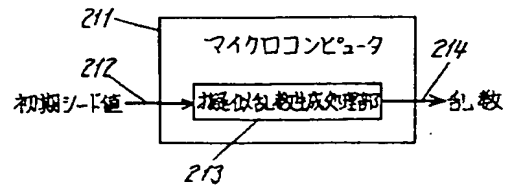
【図8】



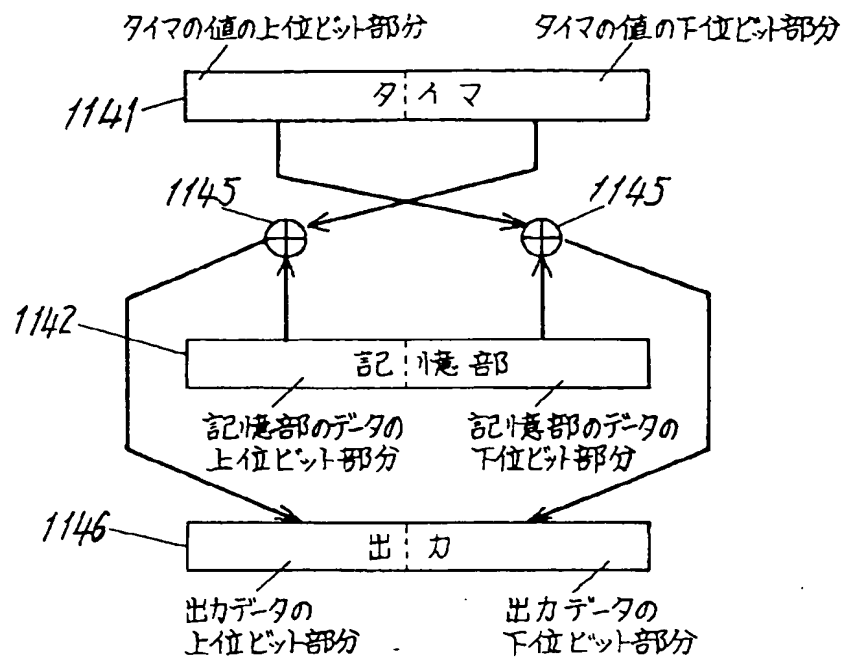
【図5】



【図9】



【図6】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.